Modeling and Verification of Insider Threats Using Logical Analysis

In this paper, we combine formal modeling and analysis of infrastructures of organizations with sociological explanation to provide a framework for insider threat analysis. We use the higher order logic (HOL) proof assistant Isabelle/HOL to support this framework. In the formal model, we exhibit and use a common trick from the formal verification of security protocols, showing that it is applicable to insider threats. We introduce briefly a three-step process of social explanation, illustrating that it can be applied fruitfully to the characterization of insider threats. We introduce the insider theory constructed in Isabelle that implements this process of social explanation. To validate that the social explanation is generally useful for the analysis of insider threats and to demonstrate our framework, we model and verify the insider threat patterns of entitled independent and Ambitious Leader in our Isabelle/HOL framework.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, Middlesex University
Contributors: Kammuller, F., Probst, C. W.
Number of pages: 12
Pages: 534-545
Publication date: 2017
Peer-reviewed: Yes

Publication Information
Journal: IEEE Systems Journal
Volume: 11
Issue number: 2
ISSN (Print): 1932-8184
Ratings:
BFI (2018): BFI-level 1
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 1
Scopus rating (2017): CiteScore 3.68 SJR 0.595 SNIP 1.847
Web of Science (2017): Impact factor 4.337
Web of Science (2017): Indexed yes
BFI (2016): BFI-level 1
Scopus rating (2016): CiteScore 3.15 SJR 0.609 SNIP 1.78
Web of Science (2016): Impact factor 3.882
BFI (2015): BFI-level 1
Scopus rating (2015): CiteScore 3.36 SJR 0.852 SNIP 2.262
Web of Science (2015): Impact factor 2.114
BFI (2014): BFI-level 1
Scopus rating (2014): CiteScore 2.92 SJR 0.747 SNIP 2.337
Web of Science (2014): Impact factor 1.98
BFI (2013): BFI-level 1
Scopus rating (2013): CiteScore 3.05 SJR 0.71 SNIP 2.018
Web of Science (2013): Impact factor 1.746
ISI indexed (2013): ISI indexed yes
BFI (2012): BFI-level 1
Scopus rating (2012): CiteScore 2.17 SJR 0.424 SNIP 1.331
Web of Science (2012): Impact factor 1.27
ISI indexed (2012): ISI indexed yes
BFI (2011): BFI-level 1
Scopus rating (2011): CiteScore 1.43 SJR 0.303 SNIP 1.124
Web of Science (2011): Impact factor 0.923
ISI indexed (2011): ISI indexed no
Web of Science (2011): Indexed yes
BFI (2010): BFI-level 1
Scopus rating (2010): SJR 0.363 SNIP 1.187
Web of Science (2010): Impact factor 0.629